Co-funded by the Erasmus+ Programme of the European Union

InCyT træningsmoduler

Informationssikkerhed for ledere **Enhed-2 Uge-3** **Enhedens navn: Informationssikkerhedsstyring -1**	
Læringsaktiviteter	❑ **Webinar** ❑ **Øvelser** ❑ **Værksted** ❑ **Præsentation** ❑ **Andet** Streaming webinar, tekst, selvevalueringsøvelser, øvelser med svar på diskussionsfora og blive diskuteret med træner/mentor
Læringsansvarlig	• Fatma Gökdemir • Ali Gökdemir
Læringsaktivitetsmål	1. Informationssikkerhed 2. Informationssikkerhedspolitikker 3. Informationssikkerhedsroller
Færdigheder, der skal opnås	• ER 1 • ER 3 • MS 3
Varighed af læringsaktivitet	2 uger
Læring krav	***Hvad skal der til?*** • Mellemliggende computerfærdigheder

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Kort information om modulet

Beskrivelse
Informationssikkerhed er af stor betydning for at sikre kontinuiteten i enhver organisation og sikrer beskyttelsen af organisationens kritiske information og andre informationsaktiver i forskellige miljøer, især elektroniske. Ikke kun store virksomheder, bedrifter, men også SMV'er, offentlige myndigheder, enhver non-profit organisation, skole eller mennesker alene oplever konstant informationssikkerhedsproblemer og -risici, om end på forskellige niveauer. I investeringer for at imødekomme disse risici er den dyreste og mest komplekse løsning ikke altid den sikreste løsning. Hver person eller organisation skal vælge og implementere den mest passende og korrekte løsning. Det skal ikke glemmes, at selvom en enkel og billig sikkerhedsløsning kan være utilstrækkelig for nogle institutioner, kan den samme løsning være tilstrækkelig og effektiv for en anden institution. Informationssikkerhed er dog ikke et arbejde, der skal startes og afsluttes. Informationssikkerhedsstyring er en livscyklus, der konstant skal styres og revideres, så længe institutioner og information eksisterer. I dette modul vil begrebet informationssikkerhed, dets betydning og hvad der bør gøres for informationssikkerhed blive forklaret. Emnet blev understøttet af et praktisk eksempel

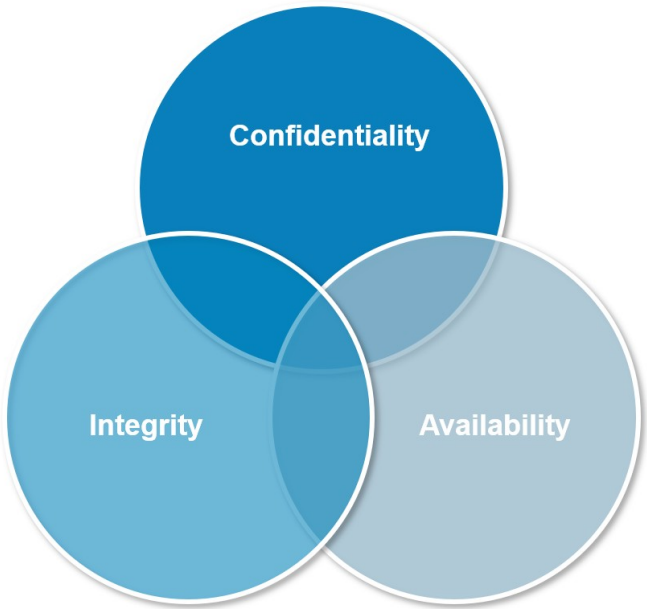
Lærematerialets indhold

1. Informationssikkerhed

Informationssikkerhed er at forhindre uautoriseret eller uautoriseret adgang, brug, ændring, offentliggørelse, ødelæggelse, udskiftning og beskadigelse af information. Den består af tre grundlæggende elementer kaldet fortrolighed, integritet og tilgængelighed (figur 1). Hvis nogen af disse tre grundlæggende sikkerhedselementer er beskadiget, opstår der en sikkerhedssårbarhed.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



Figur 1. Informationssikkerhedselementer

- Fortrolighed : Det er _ beskyttelse af oplysninger mod uberettiget adgang og uberettiget adgang .
- Integritet : Informationen ændres ikke ved uberettiget personer .
- Tilgængelighed: Information er tilgængelig og brugbar hvornår havde brug for ved autoriseret personer .

1.1. Hvad er en information sikkerhed politik ?

Sikkerhedstrusler udvikler sig konstant, og overholdelseskravene bliver stadig mere komplekse. Organisationer skal skabe en omfattende informationssikkerhedspolitik for at dække begge udfordringer. En informationssikkerhedspolitik (ISP) er et sæt regler, politikker og procedurer designet til at sikre, at alle slutbrugere og netværk i en organisation opfylder minimumskravene til it-sikkerhed og databeskyttelse. En informationssikkerhedspolitik gør det muligt at koordinere og håndhæve et sikkerhedsprogram og kommunikere sikkerhedsforanstaltninger til tredjeparter og eksterne revisorer.

1.2. Hvad er formålet med en informationssikkerhedspolitik?

En information sikkerhed politik mål til vedtage beskyttelser og begrænse _ distribution af data til kun de der med autoriseret adgang . Organisationer skab internetudbydere til :

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- Etabler en generel tilgang til informationssikkerhed
- Dokumenter sikkerhedsforanstaltninger og brugeradgangskontrolpolitikker
- Opdag og minimer virkningen af kompromitterede informationsaktiver såsom misbrug af data, netværk, mobile enheder, computere og applikationer
- Beskyt organisationens omdømme
- Overhold lovmæssige og regulatoriske krav som ENISA, NIST, GDPR, HIPAA og FERPA
- Beskyt deres kundes data, såsom kreditkortnumre
- Levere effektive mekanismer til at reagere på klager og forespørgsler relateret til reelle eller opfattede cybersikkerhedsrisici såsom phishing, malware og ransomware
- Begræns adgangen til vigtige informationsteknologiaktiver til dem, der har en acceptabel brug

1.3. Hvorfor er en informationssikkerhedspolitik vigtig?

At skabe en effektiv Information sikkerhed politik og at møder alle overholdelse krav er et kritisk skridt i forebyggelsen sikkerhed hændelser som datalæk _ og databrud . _

internetudbydere er vigtig til ny og etableret organisationer . Stigende digitalisering midler hver medarbejderen genererer data , og en del af disse data skal beskyttes _ fra uberettiget adgang . Afhængig af din industri , kan det endda være beskyttet ved love og forskrifter .

Følsomme data, personligt identificerbare information (PII), og intellektuelle ejendom skal beskyttes _ til en højere standard end andre data.

Om du kan du lide det eller ej, information sikkerhed (InfoSec) er vigtig i enhver henseende dit niveau _ organisation . Og uden for din organisation .

Informationssikkerhedspolitikker kan have følgende fordele for en organisation:

- **Letter dataintegritet, tilgængelighed og fortrolighed –** effektive informationssikkerhedspolitikker standardiserer regler og processer, der beskytter mod vektorer, der truer dataintegritet, tilgængelighed og fortrolighed.
- **Beskytter følsomme data —** Informationssikkerhedspolitikker prioriterer beskyttelse af intellektuel ejendom og følsomme data såsom personligt identificerbare oplysninger (PII).
- **Minimerer risikoen for sikkerhedshændelser — En** informationssikkerhedspolitik

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

hjælper organisationer med at definere procedurer til at identificere og afbøde sårbarheder og risici. Den beskriver også hurtige reaktioner for at minimere skader under en sikkerhedshændelse.

- **Udfører sikkerhedsprogrammer på tværs af organisationen** — Informationssikkerhedspolitikker danner rammerne for operationalisering af procedurer.
- **Giver en klar sikkerhedserklæring til tredjeparter** — Informationssikkerhedspolitikker opsummerer organisationens sikkerhedsposition og forklarer, hvordan organisationen beskytter it-ressourcer og -aktiver. De letter hurtig reaktion på tredjepartsanmodninger om oplysninger fra kunder, partnere og revisorer.
- **Hjælper med at overholde regulatoriske krav** — Oprettelse af en informationssikkerhedspolitik kan hjælpe organisationer med at identificere sikkerhedshuller relateret til regulatoriske krav og løse dem.

1.4. Hvad Bør være i en informationssikkerhedspolitik ?

En informationssikkerhedspolitik kan være svær at bygge fra bunden; det skal være robust og sikre din organisation fra alle ender. Det bør dække al software, hardware, fysiske parametre, menneskelige ressourcer, information og adgangskontrol. Det skal også være fleksibelt og have plads til revision og opdatering, og vigtigst af alt skal det være praktisk og håndhæves. Ønsketænkning hjælper dig ikke, når du udvikler en informationssikkerhedspolitik. Du skal arbejde sammen med de store interessenter for at udvikle en politik, der fungerer for din virksomhed og de medarbejdere, der skal være ansvarlige for at udføre politikken.

1. Acceptabelt Brug Politik

Denne politik beskriver den acceptable brug af computerudstyr og internettet i din organisation. Ukorrekt brug af internettet eller computere åbner din virksomhed op for risici som virusangreb, kompromitterede netværkssystemer og tjenester og juridiske spørgsmål, så det er vigtigt at have skriftligt, hvad der er og ikke er acceptabel brug.

En politik for acceptabel brug bør skitsere, hvad medarbejderne er ansvarlige for med hensyn til at beskytte virksomhedens udstyr, såsom at låse deres computere, når de er væk fra deres skrivebord eller beskytte tablets eller andre elektroniske enheder, der kan indeholde følsomme oplysninger. Det bør også skitsere, hvad virksomhedens rettigheder er, og hvilke aktiviteter der ikke er forbudt på virksomhedens udstyr og netværk.

2. Ren Skrivebord Politik

En clean desk-politik fokuserer på beskyttelse af fysiske aktiver og information. Ideelt set vil denne politik sikre, at alt følsomt og fortroligt materiale er låst væk eller på anden måde sikret, når det ikke er i brug, eller en medarbejder forlader sit skrivebord. Denne politik bør fastlægge minimumskravene for at opretholde et rent skrivebord, såsom hvor følsomme oplysninger om

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

medarbejdere, intellektuel ejendom, kunder og leverandører kan opbevares og tilgås. Det bør også dække ting som, hvilke slags materialer der skal makuleres eller smides ud, om der skal bruges adgangskoder til at hente dokumenter fra en printer, og hvilke oplysninger eller ejendom der skal sikres med en fysisk lås. Ud over at være en fælles og vigtig del af enhver informationssikkerhedspolitik, er en clean desk-politik i overensstemmelse med ISO 27001/17799 og vil hjælpe din virksomhed med at bestå en certificeringsrevision.

3. ***Databrud _ Respons Politik***

Dette er også kendt som en hændelsesplan. Formålet med en politik for bekæmpelse af databrud er at fastlægge målene og visionen for, hvordan din organisation vil reagere på et databrud. Denne plan hjælper med at mindske risikoen for at blive offer for et cyberangreb, fordi den vil detaljere, hvordan din organisation planlægger at beskytte dataaktiver gennem hele hændelsesprocessen.

Denne politik bør definere, hvem den gælder for, og hvornår den træder i kraft, herunder definitionen af et brud, personalets roller og ansvar, standarder og målinger, rapportering, afhjælpning og feedbackmekanismer.

4. ***Katastrofe Politik for genopretningsplan***

Denne politik adskiller sig fra en reaktionsplan for databrud, fordi den er en generel beredskabsplan for, hvad der skal gøres i tilfælde af en katastrofe eller enhver begivenhed, der forårsager en længere forsinkelse af tjenesten. Denne politik bør beskrive processen til at gendanne systemer, applikationer og data under eller efter enhver form for katastrofe, der forårsager et større udfald. Denne katastrofegenopretningsplan bør opdateres på årsbasis.

Beredskabsplanen bør dække disse elementer:

- Nødsituation opsøgende plan. Eksplicit liste WHO behov at blive kontaktet , hvornår gør de brug for at blive kontaktet , og hvordan vil du kontakt dem ?
- Successionsplan . Beskrive det flow af ansvar når normalt personale ikke er tilgængeligt til udføre deres pligter .
- Dataklassificeringsplan . _ Detalje alle de data, der er gemt på alle systemer , dens kritik , og dens fortrolighed .
- Servicelistens kritik . _ Liste alle det tjenester stillet til rådighed og deres rækkefølge af betydning .
- Data backup og restaureringsplan . Detalje hvilke data der er sikkerhedskopieret op , hvor og hvor ofte . _ Også forklare, hvordan dataene kan gendannes .
- Udstyr udskiftningsplan . Beskrive hvilken infrastruktur tjenester er nødvendig til Genoptag at sørge for tjenester til kunder .
- Offentlig kommunikation . Dokument WHO vilje egen det ekstern PR- funktion og give

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

retningslinjer for hvad information kan og skal deles . _

- Det er vigtig at det ledelse hold afsat tid til at teste katastrofe genopretningsplan . I løbet af Disse test også _ kendt som bordplade øvelser , den målet er at identificere problemer at er muligvis ikke indlysende i planlægning fase at kunne årsag planen om at mislykkes. Dette måde , den team kan justere planen før _ der er en katastrofe tager sted .

5. *E-mail Politik*

E-mail er en kritisk kommunikationskanal for virksomheder af alle typer, og misbrug af e-mail kan udgøre mange trusler mod sikkerheden i din virksomhed, uanset om det er medarbejdere, der bruger e-mail til at distribuere fortrolig information eller utilsigtet udsætter dit netværk for en virus. Det er vigtigt for alle medarbejdere, entreprenører og agenter, der arbejder på vegne af din virksomhed, at forstå passende e-mailbrug og at have politikker og procedurer fastlagt for arkivering, markering og gennemgang af e-mails, når det er nødvendigt.

Denne politik skal skitsere den korrekte brug af virksomhedens e-mailadresser og dække ting, såsom hvilke typer kommunikation der er forbudt, datasikkerhedsstandarder for vedhæftede filer, regler vedrørende opbevaring af e-mails, og om virksomheden overvåger e-mails. Denne politik bør også være klart udformet for dine medarbejdere, så de forstår deres ansvar i at bruge deres e-mailadresser og virksomhedens ansvar for at sikre, at e-mails bliver brugt korrekt. Denne e-mail-politik handler ikke om at skabe en "gotcha"-politik for at fange medarbejdere, der misbruger deres e-mail, men for at undgå en situation, hvor medarbejdere misbruger en e-mail, fordi de ikke forstår, hvad der er og ikke er tilladt.

6. *Slutbrugerkryptering _ _ Nøgle Beskyttelse Politik*

Visse dokumenter og kommunikationer i din virksomhed eller distribueret til dine slutbrugere skal muligvis krypteres af sikkerhedsmæssige årsager. Hav en politik på plads for at beskytte disse krypteringsnøgler, så de ikke afsløres eller bruges svigagtigt.

Denne politik bør skitsere alle krav til beskyttelse af krypteringsnøgler og angive de specifikke operationelle og tekniske kontroller på plads for at holde dem sikre. Dette inkluderer ting som manipulationssikret hardware, sikkerhedskopieringsprocedurer og hvad man skal gøre i tilfælde af, at en krypteringsnøgle mistes, stjæles eller bruges svigagtigt.

7. *Adgangskode Beskyttelse Politik*

Dine medarbejdere har sandsynligvis et utal af adgangskoder, de skal holde styr på og bruge på daglig basis, og din virksomhed bør have klare, eksplicitte standarder for at skabe stærke adgangskoder til deres computere, e-mail-konti, elektroniske enheder og ethvert punkt. adgang, de har til dine data eller netværk.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Denne politik skal også skitsere, hvad medarbejdere kan og ikke må med deres adgangskoder. Det kan virke indlysende, at de ikke skal lægge deres adgangskoder i en e-mail eller dele dem med kolleger, men du skal ikke gå ud fra, at dette er almindeligt kendt for alle. Giv dine medarbejdere al den information, de har brug for, for at skabe stærke adgangskoder og holde dem sikre for at minimere risikoen for databrud.

Endelig bør denne politik skitsere, hvad dine udviklere og it-medarbejdere skal gøre for at sikre, at alle applikationer eller websteder, der drives af din virksomhed, følger sikkerhedsforanstaltningerne for at holde brugeradgangskoder sikre.

Forskning udført i det sidste årti rundt om i verden viser, at de mest foretrukne adgangskoder for brugere er som følger:

- 123456
- adgangskode
- qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

Trods årlige advarsler har denne liste ikke ændret sig meget. Til dette rådes brugere til at følge et sæt regler for indstilling af adgangskoder. Disse regler er anført nedenfor:

- Indstilling kompleksitet krav , såsom opfyldelse _ minimumstegn _ _ krav
- Ikke at vælge tidligere Brugt adgangskoder
- Ændring adgangskoder periodisk og måske ofte
- Det adgangskoder Brugt bør ikke vælges fra almindelige og svagt Brugt adgangskoder som i liste over

National Institute of Standards and Technology (NIST) havde til formål at løse problemet med adgangskodepolitikker for at bestemme adgangskoder og opnå visse standarder. NIST angiver detaljer om adgangskoder, og hvordan de skal administreres og opbevares. Derfor bør mulige adgangskoder kontrolleres i forhold til en liste over almindeligt anvendte og kendte værdier. Overvejelser for at bestemme adgangskoder er som følger:

- Bruger leveret adgangskoder skulle gerne bestå af mindst otte alfanumerisk tegn .
- De bør ikke være adgangskoder opnået fra Tidligere brud .
- Der skal være nej ordbog ord .
- Der skal være nej datoer mellem 1900-2020 , såsom fødsel datoer .
- Ingen gentagelse eller sekventiel tegn (f.eks . aaaaaaaa eller 1234abcd)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- Ord bestemt til det tilsigtet brug , såsom navnet på tjenesten , brugernavn _ og derivater dertil bør ikke være.

Ovenstående kriterier bør tages i betragtning ved bestemmelse af adgangskoder, og adgangskoder med komplekse strukturer bør oprettes.

Adgangskodekompleksitet : Adgangskodekompleksitet er defineret som antallet af adgangskoder, der er stærke for en adgangskode, vi mener, at den opfylder et sæt regler. Nøglen til adgangskodekompleksitet Reglerne er som følger:

- Det adgangskode kan ikke indeholde det kontonavn eller _ variationer af _ kontonavn .
- Det adgangskode skal indeholde begge store bogstaver bogstaver (AZ) og små bogstaver bogstaver (az).
- Specialtegn _ **(~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /)** (Disse er det tegn at som regel komme til syne med ALT - tasten . Dog valuta _ såsom euro -symboler tæller ikke som specielle tegn).
- Minimum antal tegn _ _ skal respekteres . _ Dette værdi varierer fra system til system , bruger til bruger . kan ændre sig .

Den mindste adgangskodelængde skal være 8 tegn, mens det anbefalede tegn er 12.
Når adgangskoder oprettes med mindst 8 tegn i henhold til reglerne ovenfor, betyder det mindst 218.340.105.584.896 forskellige muligheder for en enkelt adgangskode. Sandsynligheden for den genererede adgangskode gør et brute force-angreb meget vanskeligt, men adgangskoden er stadig ikke umulig at knække. For et kodeord, der er tæt på umuligt at knække, er det nødvendigt at øge antallet af kodeordstegn. Jo højere minimumsantallet af tegn, jo længere tid tager det at knække adgangskoden.
Ud over fordelene ved adgangskodekompleksitet giver det også nogle udfordringer. En af de vigtigste er at glemme adgangskoden. Det er svært at huske en adgangskode, der er længere og indeholder specialtegn. Især når alle adgangskoder er forskellige, er det svært at huske og ikke forveksle dem med andre. Derfor bør en vis logik følges, når du opretter adgangskoder.

For eksempel;

- Jeg er det 2. barn i en familie med 3 børn !

Du kan skrive en sætning som denne baseret på dit eget virkelige liv. Når du tager de første tegn og specialtegn i sætningen, får du en adgangskode som **Iat2ciafw3c!**

- Jeg blev medlem af denne _ Hjemmeside (ca uddannelse) den 19. juli .

Du kan tilpasse en sætning som "Jeg blev medlem af denne hjemmeside (om uddannelse) den 19. juli i henhold til hjemmesidens interesseområde og datoen for medlemskab, så du ikke glemmer det. Når du får deres første karakter og specialtegn
Du får en adgangskode som **IBAMoTW (ae)oJ19.**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

8. Sikkerhedsresponsplanpolitik _ _ _

En sikkerhedsresponsplan fastlægger, hvad hvert team eller forretningsenhed skal gøre i tilfælde af en form for sikkerhedshændelse, såsom et databrud. Ifølge SANS-instituttet skal det definere "en produktbeskrivelse, kontaktoplysninger, eskaleringsstier, forventede serviceniveauaftaler (SLA), klassificering af alvorlighed og påvirkning og tidsplaner for afhjælpning/afhjælpning."

Nøglen til en sikkerhedsresponsplanpolitik er, at den hjælper alle de forskellige teams med at integrere deres indsats, så uanset hvilken sikkerhedshændelse, der sker, kan afbødes så hurtigt som muligt. Selvom hver afdeling kan have sine egne responsplaner, beskriver sikkerhedsresponsplanens politik, hvordan de vil koordinere med hinanden for at sikre, at responsen på en sikkerhedshændelse er hurtig og grundig.

1.5. Informationssikkerhedspolitik _ Eksempler

For at skabe en vellykket cybersikkerhedsplan skal 5 hovedspørgsmål overvejes.

a. ***Identificer :*** Det organisation skulle gerne har forståelse for _ _ cybersikkerhed risici det står over for så den kan prioritere dens indsats .

b. ***Beskyt*** : Det handler om sætte passende sikkerhedsforanstaltninger på plads til beskytte dataaktiver _ og begrænse eller indeholde det effekt af et potentiale cybersikkerhed begivenhed . Dette omfatter uddanne og bemyndigende personale medlemmer inden for det organisation at være opmærksom på risici , etablere procedurer at fokus på at beskytte netværkssikkerheden og aktiver , og potentielt udnytter cyber ansvar forsikring til beskytte en virksomhed økonomisk i _ begivenhed en cyberkriminel er i stand til at omgå _ beskyttelser at er på plads .

c. ***Opdag*** : Omrids det aktiviteter at hjælpe med at opdage det forekomsten af en cyber angreb og aktivere rettidigt respons til det begivenhed . I bestille til hurtigt og effektivt diagnosticere en cyber angreb , virksomheder skulle gerne implementere dataklassificering , aktiv _ ledelse og risikostyring _ _ protokoller at alert dem når data vises at blive kompromitteret .

d. ***Svar*** : Dokument det passende handlinger at bør tages _ følge det afsløring af cybersikkerhed trusler . En virksomheds respons skulle gerne omfatte passende og grundig meddelelse med medarbejdere , aktionærer , partnere og _ kunder såvel som med _ lov håndhævelse og juridisk rådgivning efter behov .

e. ***Recover*** : Bestem , hvordan en organisation kan komme sig og genskabe evt

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

kapaciteter eller tjenester at var svækket på grund til en cyber angreb .

Næsten alle sikkerhedsstandarder skal indeholde et krav om en eller anden type hændelsesresponsplan, fordi selv de mest robuste informationssikkerhedsplaner og overholdelsesprogrammer stadig kan blive ofre for et databrud.

1.6. Øvelser af informationssikkerhedspolitik

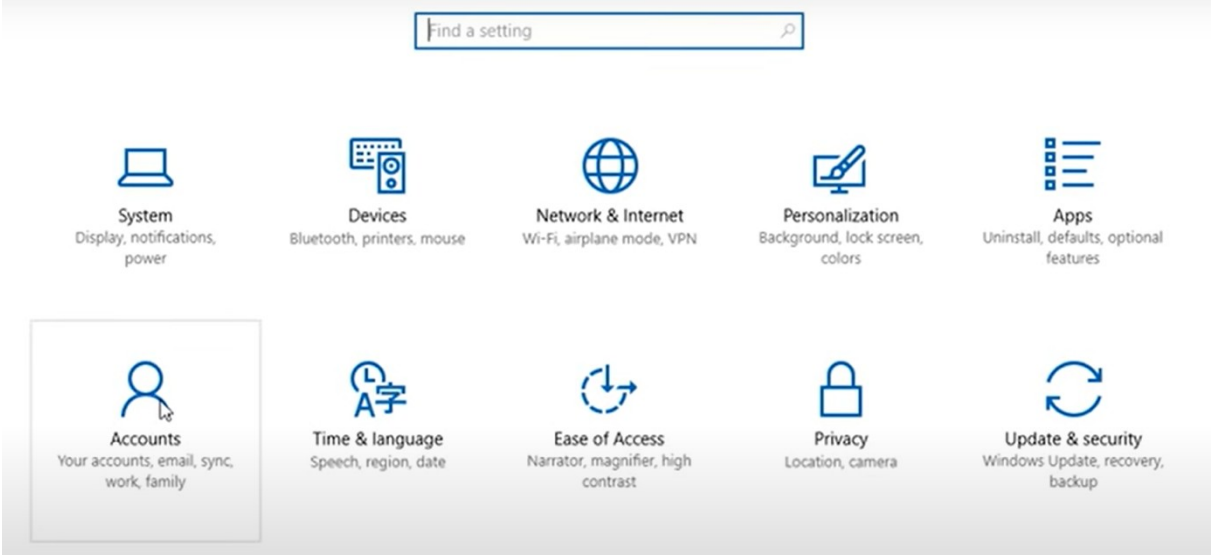
1. Lås din session: Styrk dine onlinekonti ved at aktivere de stærkeste tilgængelige godkendelsesværktøjer, såsom biometri (en persons målbare biologiske spor), sikkerhedsnøgler eller en unik engangskode genereret af et applikationsværktøj på din mobilenhed. Dine brugernavne og adgangskoder er muligvis ikke tilstrækkelige til at beskytte konti som e-mail, bank og sociale medier.

Øvelser-1:

For at få computeren til at låse automatisk, når du rejser dig fra computeren.

Trin-1: Klik på knappen Windows-indstillinger.

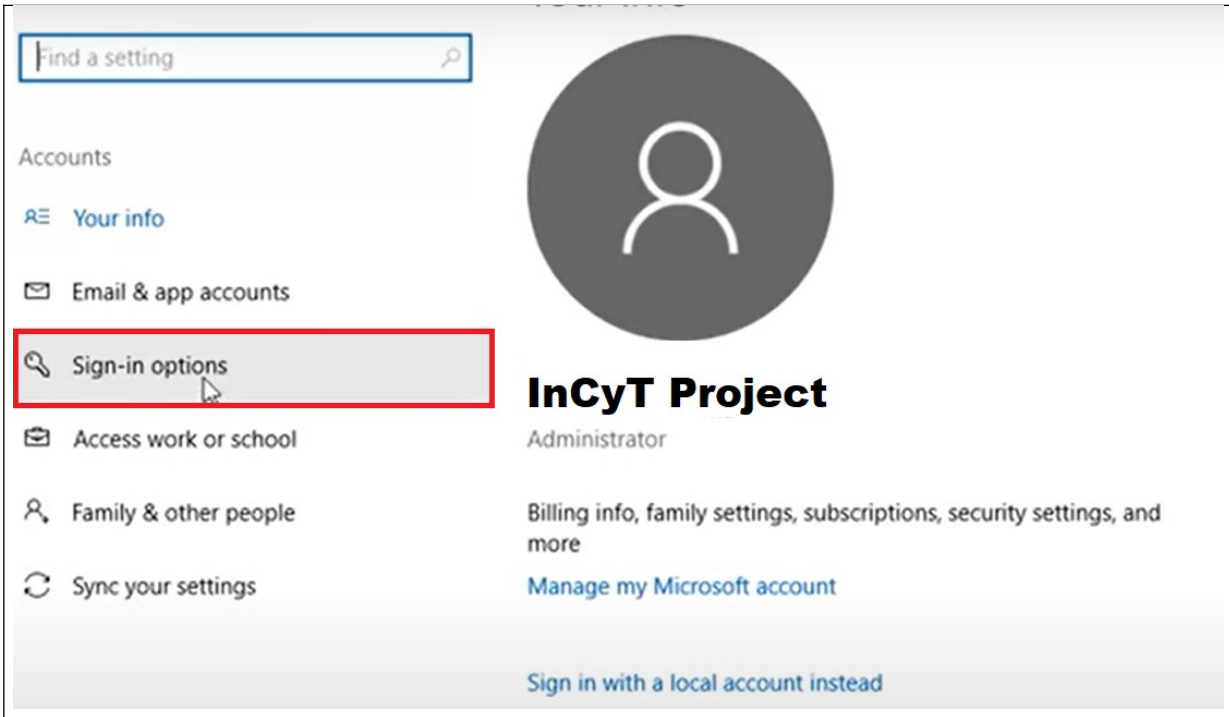
Trin-2: Klik på fanen Konti.



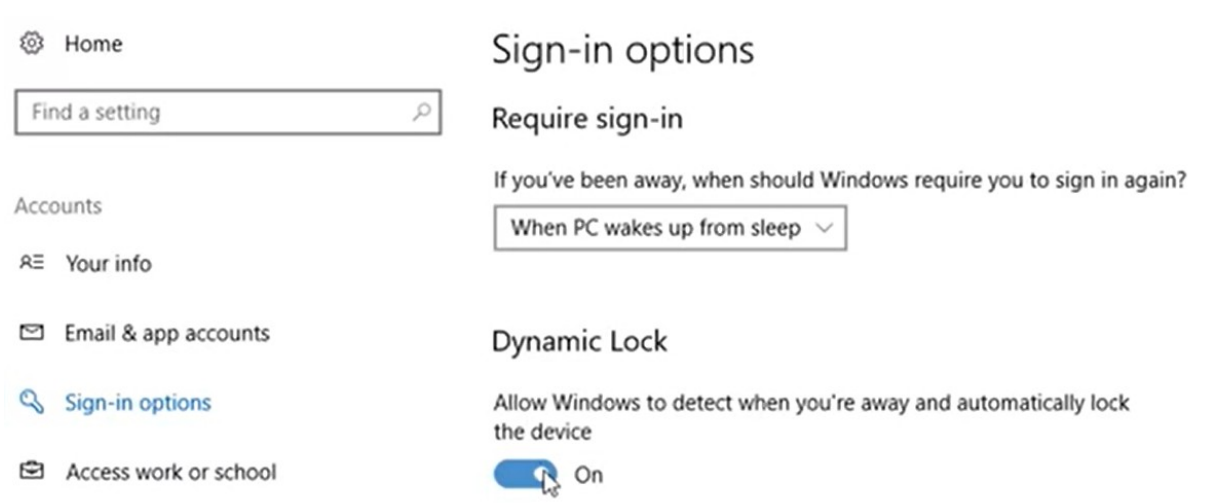
Trin-3: Klik på sektionen Log ind.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



Trin-4 : Aktiver til Dynamic Lock -specifikationen .



2- Opret en stærk adgangskode: Adgangskode har en vigtig plads i informationssikkerheden. Svage adgangskoder kan løses på kort tid med programmer til at knække adgangskoder. Af denne grund er det nødvendigt at tage den største omhu ved at overveje følgende regler, når du opretter og bruger adgangskoder på alle enheder og konti. Adgangskoden bruges generelt mange steder i computersystemer. Vi bruger en adgangskode, når vi opretter en e-mail-konto, sætter en adgangskode på computerens login og forbyder adgang til filer. Adgangskoder bør dog

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

ikke være svage eller gættelige. Adgangskoder skal oprettes i henhold til følgende kriterier:

a. Adgangskoder skal være på ***mindst 8 tegn*** lang og indeholde mindst _ en store bogstaver brev , et små bogstaver brev , et nummer , og en særlig tegn (.-+=_,! @$#*%<>[]{}).
b. Det adgangskode Mark ***bør ikke være*** venstre blank eller standard ; ***123456, 01062022, qwerty , adgangskode osv .*** det bør ikke bestemmes på en sådan måde at det er forudsigeligt og let gået i stykker synes godt om ord der kan findes i enhver ordbog .
c. Adgangskoder skulle gerne **ikke indeholde personlig oplysninger** (din barnets navn , fødselsdato eller _ _ institutionens navn).
d. ***Forskellige adgangskoder*** skal oprettes _ til forskellige systemer og regnskaber .
e. Adgangskoder bør ændres _ ofte (mindst hver 6. måned).
f. Adgangskoder skulle gerne ***ikke skrives*** steder _ der kan mærkes ved Andet mennesker (såsom at forlade dem Næste til det computer ved skrive på papir) og bør ikke opbevares klar _ tekst uden kryptering på en computer eller i nogen digital medium .
g. Intet personale eller studerende skulle gerne ***del*** deres adgangskode (e-mail-adgangskode , e - signatur adgangskode , pc- adgangskode osv .) med en anden person . Brugere skulle gerne ved godt at alt juridisk ansvar at kan opstå i tilfælde af deling vilje tilhører til ham .
h. Enestående konto , unik adgangskode : At have en separat adgangskode til hver konto hjælper modarbejde cyberkriminelle . Hos _ meget mindst adskille _ din arbejde og personlig regnskaber og sørg for din kritisk regnskaber har det stærkeste adgangskoder .
i. Husk og hold det sikkert : Stærk adgangskoder er svært til skab og huske . Indstil din adgangskoder på en måde det er meningsfuldt og mindeværdig kun til dig , eller holde dem i et pengeskab placere og format. Alternativt kan du bruge en tjeneste såsom en adgangskode Manager til holde spore din _ adgangskoder .

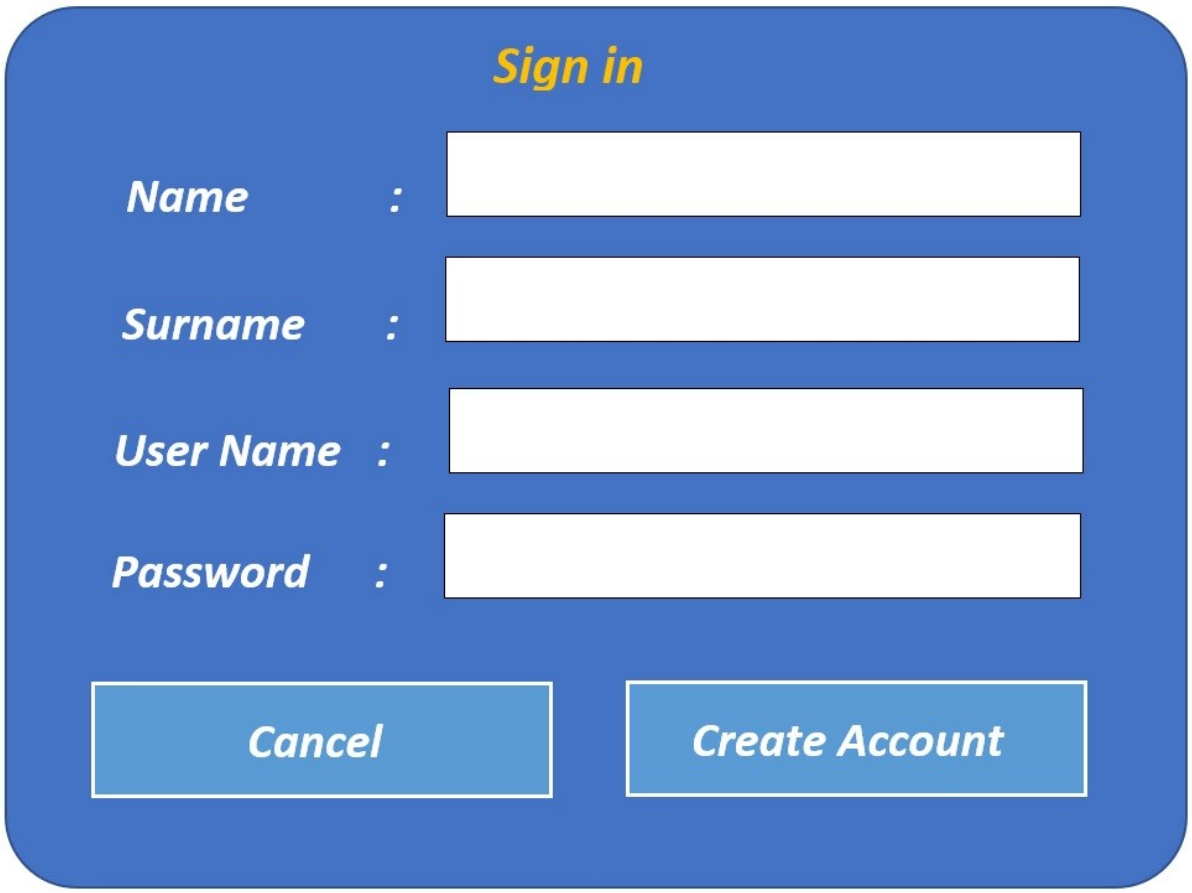
Øvelser-2 :

Adgangskodesikkerhed, når du opretter en e-mail-konto gennem din virksomheds e-mail-tjenesteudbyder eller en offentlig e-mail-tjenesteudbyders applikation eller websted

Trin-1: Åbn webstedet eller applikationen.
Trin-2: Indtast dine personlige oplysninger for at oprette en konto.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



Trin-3: Når du opretter en adgangskode, skal du bruge store bogstaver, små bogstaver, ciffer, symbolkombinationer sammen.
Nogle kodninger kan udføres for at gøre adgangskoden let at huske for brugeren. For eksempel kan du skrive en sætning, der passer til emnet, og bruge de første tegn, tal og specialtegn i den sætning, du skrev.

D hans **cybersikkerhedsprojekt** er støttet af **E** rasmus **+** _ _ _ _ _ _ **2021**

Trin-4: Vi sætter vores adgangskode; TcpisbE+2021

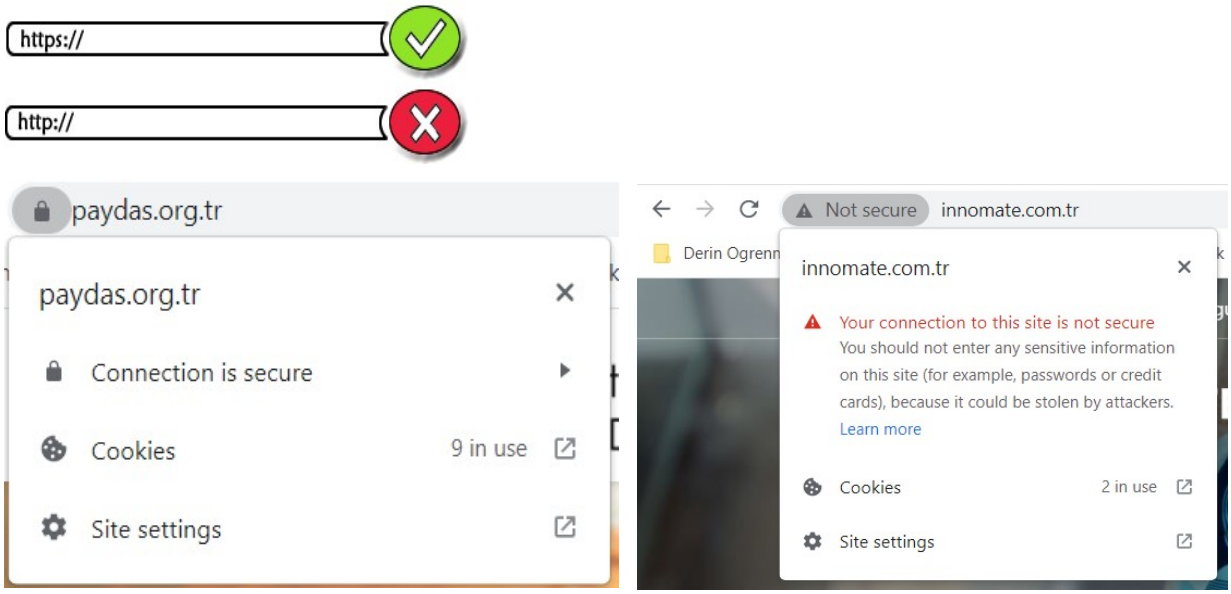
Trin-5: Sørg for, at adgangskoden består af mindst 8 tegn. 12 tegn foretrækkes. Det kan siges, at den adgangskode, vi bruger, er egnet, fordi den har 12 tegn.

3- Adgang til sikre websteder (Sikker browser) : Når du går online for at shoppe eller læse nyheder, bruger du en browser. Browsere er en af de primære måder at interagere med

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

internettet på. Som følge heraf er browsere primære mål for cyberangribere. Brug altid den nyeste version af din browser og hold dit sikkerhedsskjold stærkt mod browserangreb. Opdaterede browsere har de nyeste sikkerhedsrettelser og er meget sværere for cyberangribere at udnytte. Ikke sikker på, om du har den seneste browseropdatering? Kontakt det tekniske supportteam eller informationssikkerhedsteamet for at bekræfte. Hold dig sikker online ved ikke at oprette forbindelse til websteder, når du modtager en advarsel fra din browser. Moderne browsere kan genkende visse ondsindede websteder, der er designet til at skade. Hvis din browser giver dig besked om, at det websted, du er ved at besøge, er farligt, skal du lukke denne webside og prøve at finde den information, du leder efter, på et mere sikkert websted. Før du sender følsomme oplysninger online, for eksempel når du sender dine kreditkortoplysninger til online shopping, skal du sikre dig, at din browser bruger HTTPS, som er et tegn på kryptering. Kryptering blander de oplysninger, der transmitteres mellem din computer og destinationen, så kun den autoriserede hjemmeside kan læse den. For en sikker forbindelse skal du se efter krypteringsmærker såsom webstedsadressen, der starter med HTTPS, og et hængelåsikon i statuslinjen.



Figur 2. Sikre og ikke sikre websteder

tilføjelser; er små stykker software tilføjet til browsere, der bruges til yderligere funktioner såsom at spille spil, se film eller redigere tekst. Hver tilføjelse installeret i din browser tilføjer potentielt yderligere sikkerhedssårbarheder. Hvis du absolut har brug for dem og kun med forudgående godkendelse, skal du installere tilføjelserne i din browser. Når det er installeret, skal du altid bruge den nyeste version af pluginnet, ligesom i din browser. Til sidst, når du er færdig med at besøge et websted, skal du sørge for, at du er logget ud. Dette fjerner følsomme login- og adgangskodeoplysninger, før du lukker browseren. Husk, din sikker browsing-adfærd

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

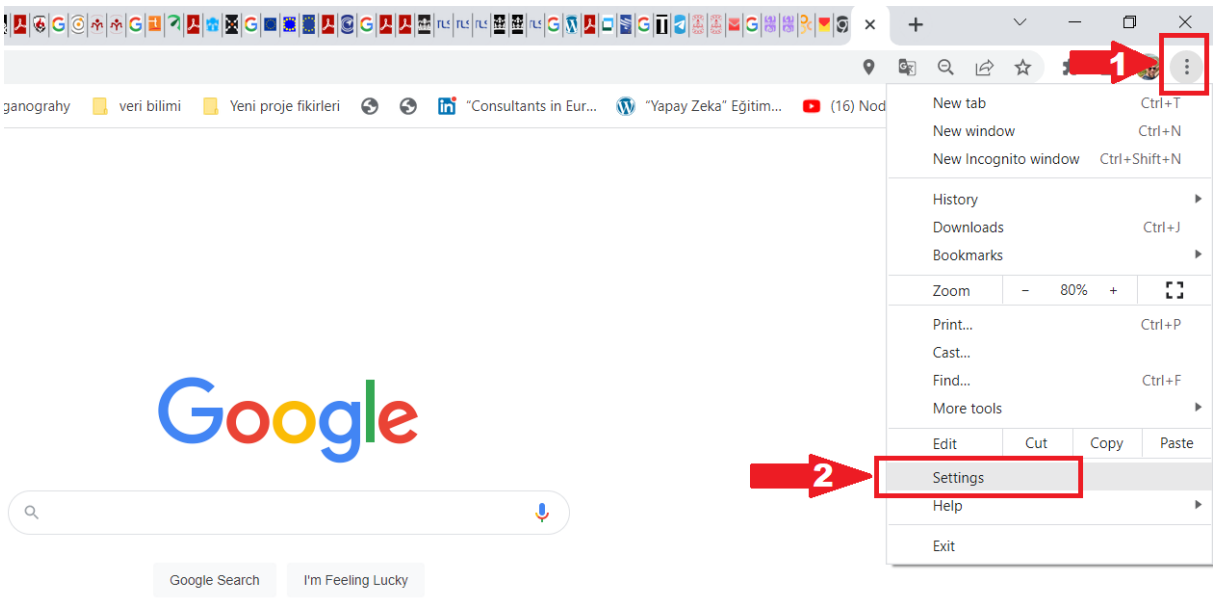
Co-funded by the Erasmus+ Programme of the European Union

og sikkerhedsskjold er styrket.

Øvelser-3:

Følg nedenstående trin for at redigere plug-ins i webbrowseren.

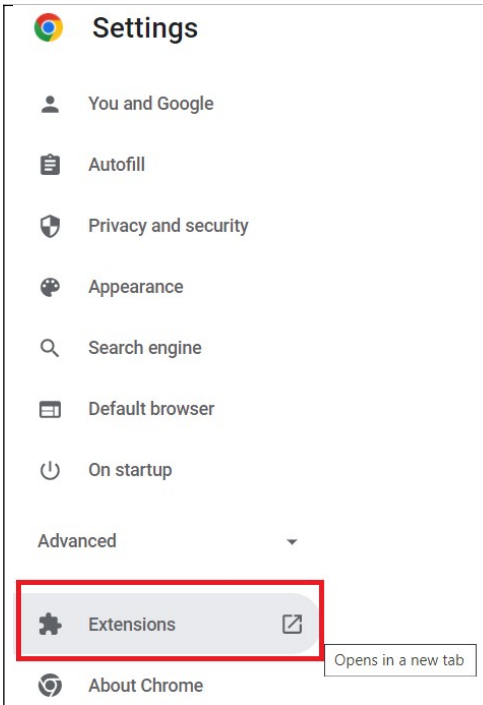
Trin-1: Åbn din webbrowser, og klik på knappen "Kostume og kontrol..." i øverste venstre hjørne (1). Klik på fanen "Indstillinger" fra rullemenuen (2).



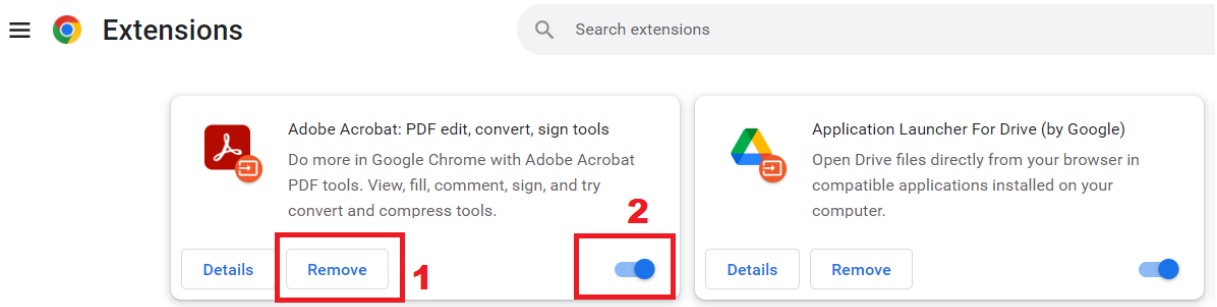
Trin-2: Klik på knappen "Udvidelser" i det vindue, der kommer op.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



Trin-3: Du kan se tilføjelserne installeret på din browser på denne skærm. Hvis du vil slette tilføjelsen, kan du slette den (1) ved at trykke på knappen "Fjern". Hvis du ønsker, at plugin'et skal forblive inaktivt, kan du deaktivere det fra "On-Off"-knappen (2).



4. E-mail, beskeder og phishing : Hav en e-mail i din indbakke eller en besked på din telefon. "Der er et problem med din konto, og din konto bør opdateres med det samme. Alt du skal gøre er at klikke på et link." Når du får en besked med indhold, så stop op og tænk dig om, før du klikker! "Phishing" er et socialt ingeniørangreb, der bruger e-mails eller beskeder som lokkemad, som at bruge agn til fiskeri. Cyberangribere sender tusindvis af e-mails i håb om, at nogen vil tage agnen. E-mails beder dig om at foretage en handling, såsom at klikke på et link, åbne en vedhæftet fil eller udfylde en formular. Cyber angribere er ikke sikre på, præcis hvem der vil modtage disse e-mails, men at udføre en af disse tilsyneladende harmløse handlinger kan få dig

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

til at blive hooked. En mere sofistikeret form for phishing kaldet "Spear phishing" retter sig mod bestemte personer. For eksempel, når alle i vores organisation modtager en generisk phishing-e-mail vedrørende en ikke-leveret pakke; ligesom fem personer i vores indkøbsenhed bliver målrettet med en falsk fakturaanmodning. Hvordan ved vi, om en e-mail eller besked er et phishing-angreb?

Nogle tegn at kigge efter:

- Beskeder starten med " Kære Kunde ” eller anden generel hilsen indgange .
- Beskeder at kræve umiddelbar handling eller skabe en følelse af at det haster , såsom truende til tæt din konto .
- Beskeder at påstand at være fra en embedsmand organisation, men har grammatisk eller stavning fejl eller bruge en personlig e-mail adresse såsom @gmail.com, @yahoo.com eller @hotmail.com.
- Nogen besked at spørger til højt følsom oplysninger , såsom din _ kredit kort nummer eller adgangskode . Vær mistænksom over for sådan beskeder . Hvis nogen du kender , såsom en kollega , sender dig en besked at kræver presserende handling , rækkevidde ud igennem forskellige kanaler til verificere at det virkelig er Hej M hvem sendte dig , for eksempel ved telefon opkald Prøve til bekræfte hvis det besked er hans.

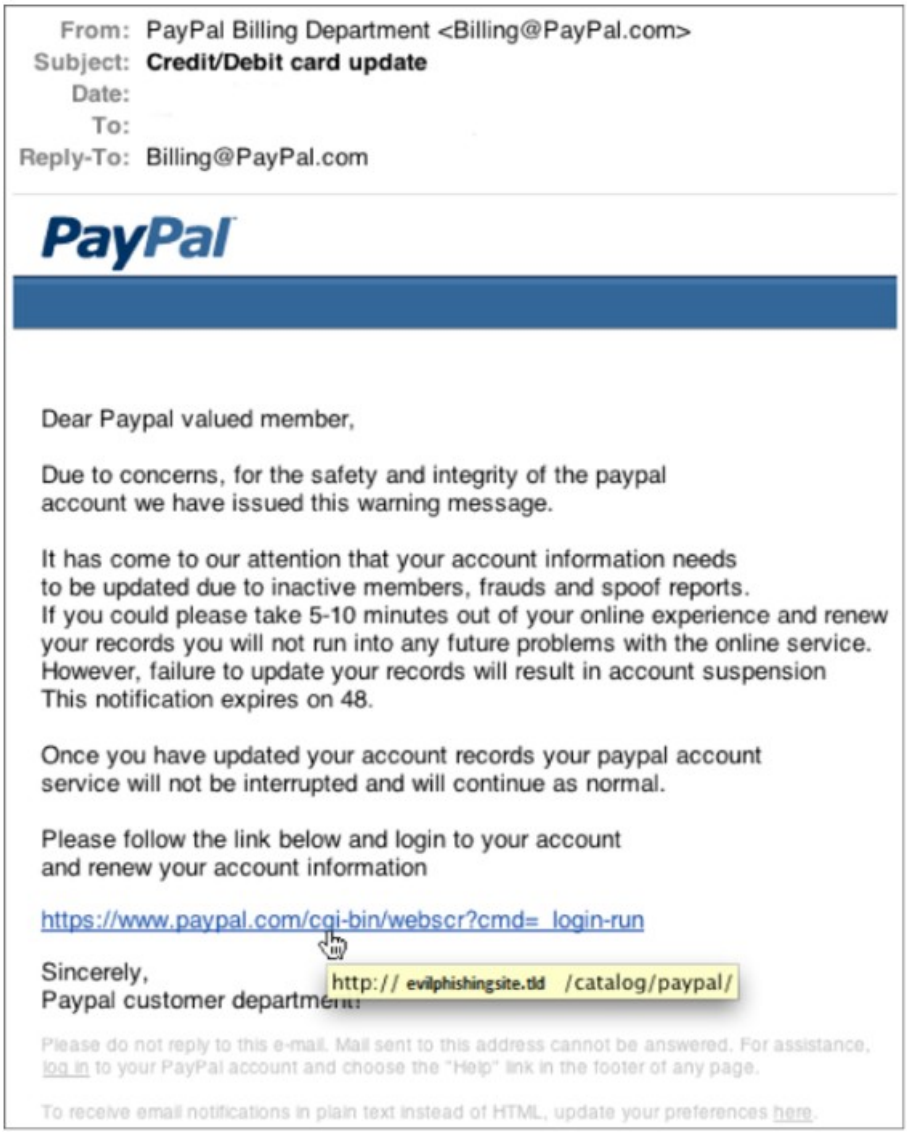
Husk, det er meget nemt for en cyberangriber at oprette en e-mail, der ser ud som om den kom fra en ven eller kollega. For at være sikker bør du altid tage disse forholdsregler, når du bruger e-mail eller beskeder. Hold musen over et link, før du klikker på det. Dette vil vise den sande destination for linket, så du kan bekræfte, at du er blevet omdirigeret til et legitimt websted. Endnu bedre er det at indtaste hjemmesidens adresse direkte i din browser. Hvis du f.eks. modtager en e-mail fra din bank, der beder dig om at opdatere kontooplysningerne, skal du ignorere det e-mailede link. Du skal blot indtaste din banks hjemmesideadresse i din browser og logge ind som normalt. Når meddelelser har vedhæftede filer, skal du kun åbne vedhæftede filer, som du forventer. Fordi antivirusløsninger muligvis ikke registrerer alle versioner af malware, er du det bedste forsvar, vi har mod inficerede vedhæftede filer. Når du bruger e-mail eller beskeder, skal du passe på ikke at afsløre vigtige oplysninger ved et uheld. E-mail-funktioner som autofuldførelse gør det nemt utilsigtet at sende e-mail til den forkerte person. For eksempel, når du vil sende en e-mail til en person, der arbejder i din enhed, kan du ved et uheld sende en e-mail til en ven med et lignende navn, der arbejder i en anden enhed. Husk, at når først en e-mail er sendt, er den ude af din kontrol.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Eksempler på phishing

Eksempel-1: I dette eksempel ser e-mailen ud, som om den er sendt fra PayPal.com, men sendes via en falsk server. Hvis vi kun ser på den webadresse, som den er rettet til, uden at klikke på det givne link, kan vi opdage, at det er en e-mail, der er høstet af en angriber, der ønsker at indhente legitimationsoplysninger.



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date:
To:
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http:// evilphishingsite.tld /catalog/paypal/

Sincerely,
Paypal customer department

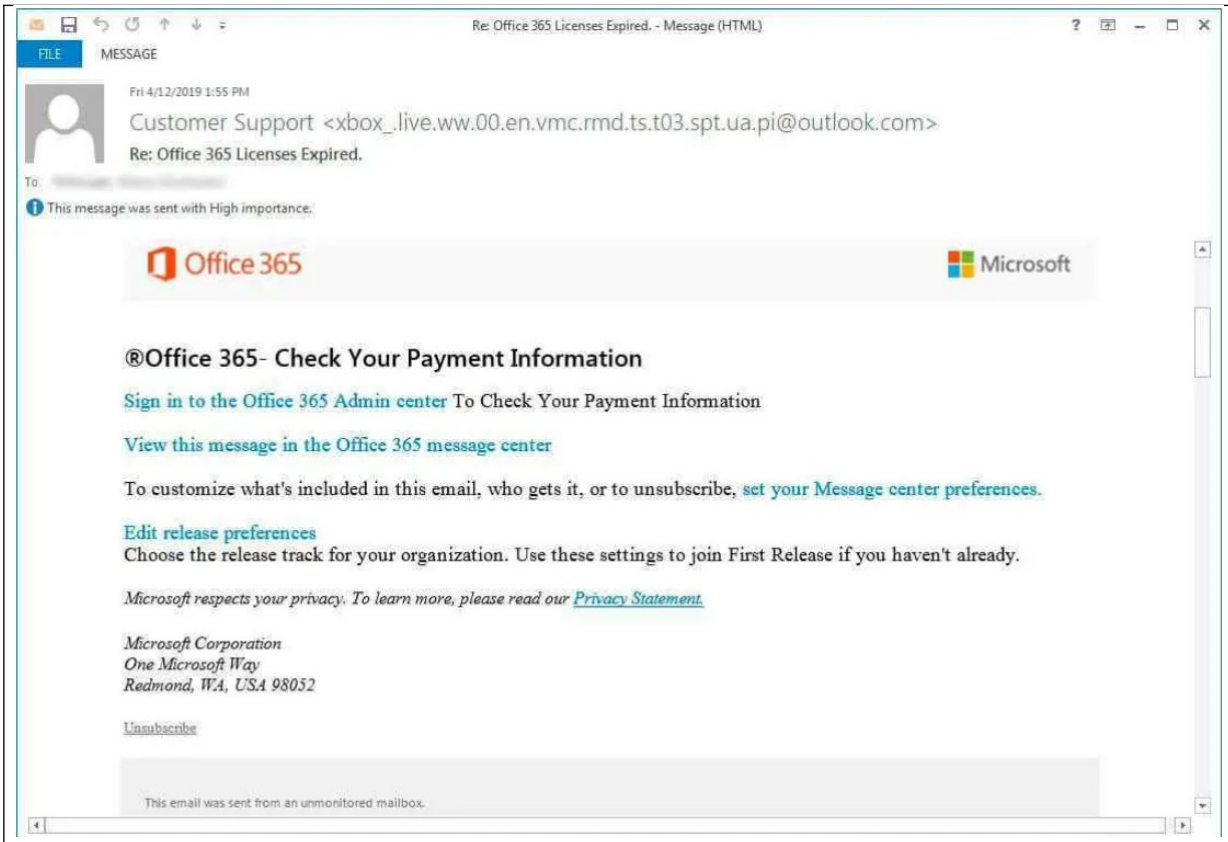
Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

Eksempel-2 : I dette eksempel er en indgående e-mail et eksempel, der indikerer, at en organisations Office 365-licenser er udløbet. Mailen bliver derefter ved med at fortælle brugeren om at logge ind på Office 365 Admin Center for at tjekke deres betalingsoplysninger.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



Men når afsenderens e-mailadresse undersøges nøje, skal det bemærkes, at en sådan adresse ikke vil eksistere. Kort sagt er det indlysende, at denne e-mail ikke blev sendt af Office365.

5. Sociale netværk

Sociale netværkssider hjælper os med at dele information og kommunikere med andre. Desværre gør disse websteder det også nemmere for cyberangribere at spore dig og lære, hvad du laver. Beskyt dig selv ved at beskytte hver konto med en stærk, unik adgangskode. Endnu bedre, brug en anden adgangskode for hver konto og brug to-faktor-godkendelse, hvis den er tilgængelig. Mange sociale netværkssider understøtter også tredjepartsapps. Installer kun apps, du har brug for, fra pålidelige kilder og kun. Tjek enhver apps vurdering, kommentarer og tilladelser, før du installerer den. Hvis du ikke længere har brug for en app, skal du afinstallere den eller deaktivere dens adgang til din sociale netværksprofil.

Ligesom e-mail og meddelelser kan cyberangribere forsøge at snyde dig på sociale netværkssider. Han kan sende beskeder og udgive sig for at være din ven. Hvis du modtager en mærkelig eller mistænkelig besked fra en ven, skal du kontakte vedkommende via e-mail eller telefon, ikke ved at svare på beskeden. Endelig, for at beskytte vores institution, må du ikke

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

poste nogen fortrolige oplysninger om vores institution på nogen hjemmeside. Hvis du har spørgsmål til, hvad du kan poste eller dele om jobbet, så spørg venligst din vejleder.

Efter aktivering af to-faktor-godkendelse (bekræftelse), vil en sikkerhedskode blive sendt til din telefon eller godkendelsesapp, hver gang du logger ind på din konto fra en ny enhed eller browser. Du skal indtaste denne kode, og du får lov til at logge ind. Hvis en cyberkriminel forsøger at logge ind på din konto, kan de ikke gøre det, hvis de ikke har adgang til din mobiltelefon. Du vil også kunne bemærke et forsøg på at logge ind på din konto, da du vil modtage en notifikation med en kode. Del aldrig denne kode med andre! En angriber vil prøve at tage den. Hvis du har modtaget koden, men ikke forsøgte at logge ind, skal du slette kodemeddelelsen og ændre din adgangskode så hurtigt som muligt.

Øvelser-4:

Udfør to-faktor autentificering- bekræftelse for at få adgang til den e-mail-konto, du har oprettet. Den første af disse processer er den adgangskode, du bruger til at få adgang til kontoen. Den anden kan være en bekræftelseskode (SMS), der skal sendes til din telefon eller et bekræftelseslink, der skal sendes til en anden e-mailadresse.

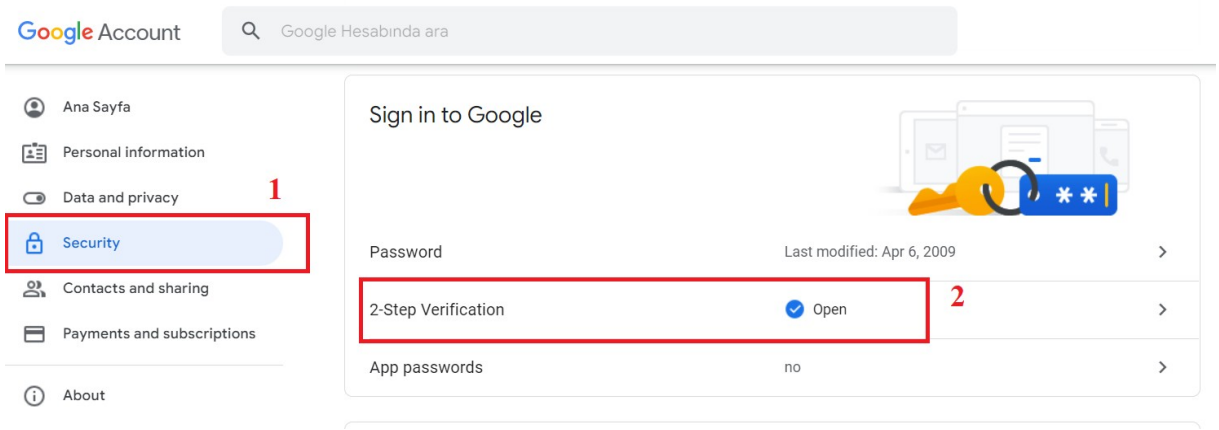
Skærmbilledet nedenfor viser, hvordan du aktiverer to-faktor-godkendelsesfunktionen på Gmail-kontoen.

Fuldfør processen, og prøv at få adgang til din e-mail-konto igen.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Trin-1 : Åbn din Google-konto.
Trin-2: Klik til afsnittet "Indstillinger".
Trin-3: Vælg fanen "Sikkerhed" fra menuen til venstre på siden, der åbnes (1). Aktiver derefter funktionen "2-trinsbekræftelse" midt på siden.



1.7. Bedste praksis for vellykkede informationssikkerhedspolitikker

1. **Information og dataklassificering:** Kan lave eller ødelægge dit sikkerhedsprogram. Dårlig information og dataklassificering kan efterlade dine systemer åbne for angreb. Derudover kan mangel på ineffektiv styring af ressourcer medføre overheadudgifter. En klar klassifikationspolitik hjælper organisationer med at tage kontrol over fordelingen af deres sikkerhedsaktiver.
2. **IT-drift og administration:** Bør arbejde sammen for at opfylde compliance- og sikkerhedskrav. Manglende samarbejde mellem afdelinger kan føre til konfigurationsfejl. Teams, der arbejder sammen, kan koordinere risikovurdering og identifikation gennem alle afdelinger for at reducere risici.
3. **Responsplan for sikkerhedshændelser:** Hjælper med at igangsætte passende afhjælpningshandlinger under sikkerhedshændelser. En sikkerhedshændelsesstrategi giver en retningslinje, som inkluderer indledende trusselsrespons, prioritetsidentifikation og passende rettelser.
4. **SaaS og cloud-politik** – giver organisationen klare retningslinjer for cloud og SaaS-vedtagelse, som kan danne grundlaget for et samlet cloud-økosystem. Denne politik kan hjælpe med at afbøde ineffektive komplikationer og dårlig brug af cloud-ressourcer.
5. **Acceptable use policies (AUP'er):** Hjælper med at forhindre databrud, der opstår ved misbrug af virksomhedens ressourcer. Gennemsigtige AUP'er hjælper med at holde alt personale på linje med den korrekte brug af virksomhedens teknologiressourcer.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

6. **Politik for identitetsadgang og -administration (IAM):** Skitserer, hvordan it-administratorer godkender systemer og applikationer til de rigtige medarbejdere, og hvordan medarbejdere opretter adgangskoder for at overholde sikkerhedsstandarder. En simpel adgangskodepolitik kan reducere identitets- og adgangsrisici.
7. **Datasikkerhedspolitik:** Skitserer de tekniske krav og acceptable minimumsstandarder for datasikkerhed for at overholde relevante love og regler
8. **oplysninger** : Offentligt håndhævede regler, såsom den generelle databeskyttelsesforordning (GDPR) beskytter slutbrugeres privatliv . Organisationer, der ikke beskytter deres brugeres privatliv, risikerer at miste deres autoritet og kan blive idømt bøder.
9. **Politik for personlige og mobile enheder:** Skitserer, om medarbejdere har tilladelse til at bruge personlige enheder til at få adgang til virksomhedens infrastruktur, og hvordan man kan reducere risikoen for eksponering fra medarbejderejede aktiver. I dag er de fleste organisationer flyttet til skyen. Virksomheder, der opfordrer medarbejdere til at få adgang til virksomhedens softwareaktiver fra et hvilket som helst sted, risikerer at introducere sårbarheder gennem personlige enheder såsom bærbare computere og smartphones. Oprettelse af en politik for korrekt sikkerhed af personlige enheder kan hjælpe med at forhindre eksponering for trusler via medarbejderejede aktiver.
10. **Fjernadgangspolitik** : Skitserer acceptable metoder til fjernforbindelse til interne netværk
11. **mail/kommunikationspolitik** : Skitserer, hvordan medarbejderne kan bruge virksomhedens valgte elektroniske kommunikationskanal såsom e-mail, slack eller sociale medier
12. **Disaster recovery policy** : Skitserer organisationens cybersikkerhed og it-teams input til en overordnet forretningskontinuitetsplan
13. **Forretningskontinuitetsplan (BCP):** Koordinerer indsatsen på tværs af organisationen og bruges i tilfælde af en katastrofe til at genoprette virksomheden til en funktionsdygtig stand
14. **Utilsigtet hændelse respons (IR) politik** : En organiseret nærme sig til hvordan _ organisation vilje styre og afhjælpe en hændelse
15. **Lave om ledelse politik** : Henviser til det formel behandle til fremstilling ændringer til IT, softwareudvikling og sikkerhed

Spørgsmål :

1- Som ikke er en af de Information sikkerhed elementer ?

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

A) Fortrolighed

B) Integritet

C) Sårbarhed

D) Tilgængelighed

2- Hvilken af _ følgende er ikke en af de institutioner at bestemme Information sikkerhed politik ?

A) ENISA

B) IPA

C) GDPR

D) NIST

3- Hvilken af _ følge fordele ikke direkte _ har Information sikkerhed politikker for en organisation ?

A) Beskyttelse følsomme data

B) Minimering risikoen for sikkerhed hændelser

C) Giver en klar sikkerhedserklæring _ _ til tredje fester

D) Reducerende det arbejder medarbejdernes timer _

4- Hvilken af _ følgende er ikke inkluderet i oplysningerne sikkerhed

A) Hardwarepolitik

B) E-mail Politik

C) Katastrofe Politik for genopretningsplan

D) Adgangskode Beskyttelse Politik

5- Hvilken af _ følge ville være et eksempel på en veldefineret adgangskode ?

A) 20220829

B) InCyT#2021!

C) Erasmus +

D) 123456!

6- Hvilken af _ følgende er ikke en af de foranstaltninger skal tages _ til Information sikkerhed ?

A) Foretrækker https websider _

B) Brug af en stærk adgangskode

C) Besøg links af ukendte oprindelse

D) Ser på computer skærmen højst 8 timer om dagen _ _

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Selvevalueringsspørgsmål. Efter besvarelsen kan eleven se resultaterne og sammenligne dem med disse gemt på platformen

- ***Hvorfor er en informationssikkerhedspolitik vigtig ?***
- ***Forklare det adgangskode Beskyttelse Politik***

Vedhæftede filer *(PowerPoint-præsentation, uddelingskopier, udskrifter, links, video...):*

Referencer:

http://bid.ankara.edu.tr/2018/10/02/siber-guvenlik-farkindaligi/
https://purplesec.us/resources/cyber-security-policy-templates/#Email
http://ix-one.com/domainhostingFAQ/article/MS_27805.html
https://www.siberguvenlik.web.tr/index.php/2019/07/22/kimlik-avcilari-sahte-yonetici-uyarilari-ile-office-365-yoneticilerini-hedefliyor/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.